AMENDMENTS TO THE CLAIMS:

Please cancel Claims 1-120 and 167-174 without prejudice or disclaimer of the subject matter thereof.. This listing of claims will replace all prior versions and listings of claims in the above-referenced application.

Listing of Claims:

1. – 120. (Canceled)

121. (Original) A method for monitoring an industrial network comprising:

reporting first data about a first computer system by a first agent executing on said first computer system in said industrial network, said first computer system performing at least one of: monitoring or controlling a physical process of said industrial network, said first data including information about software used in connection with said physical process.

122. (Original)The method of Claim 121, further comprising:

reporting second data about communications on a connection between said industrial network and another network by a second agent executing on a second computer system.

123. (Original)The method of Claim 122, wherein said second data reported by said second agent is included in an appliance to which said first data is sent.

124. (Original)The method of Claim 121, wherein said first agent reports on at least one of: critical file monitoring, log file for said first computer system, hardware and operating system of said first computer system, password and login, a specific application executing on said computer system wherein said application is in accordance with a particular industrial application of said industrial network.

125. (Original)The method of Claim 124, wherein a plurality of agents execute on said first computer system monitoring said first computer system.

126. (Original) The method of Claim 125, wherein said plurality of agents includes a master agent and other agents performing a predetermined set of monitoring tasks, said master agent controlling execution of said other agents.

127. (Original)The method of Claim 126, wherein said plurality of agents report data at predetermined intervals to one of: an appliance and said second computer system.

128. (Original) The method of Claim 127, further comprising performing, by at least one of said plurality of agents:

obtaining data from a data source;

parsing said data;

performing pattern matching on said parsed data to determine events of interest;

recording any events of interest;

reporting any events of interest in accordance with occurrences of selected events

in a time interval;

creating a message including said summary at predetermined time intervals; and

encrypting at least one of: said message and a checksum of said message.

129. (Original)The method of Claim 121, wherein said first data includes at least one of the following metrics: a number of open listen connections and a number of abnormal process terminations.

130. (Original) The method of Claim 129, wherein, when a number of open listen connections falls below a first level, an event corresponding to a component failure is determined.

131. (Original) The method of Claim 129, wherein, when a number of open listen connections is above a second level, an event corresponding to a new component or unauthorized component is determined.

132. (Original)The method of Claim 122, wherein said second agent reports on network activity in accordance with a set of rules, said rules including at least one rule indicating that events in a business network are flagged as suspicious in said industrial network.

133. (Original)The method of Claim 132, wherein said events include at least one of: an event associated with a web browser, and an event associated with e-mail.

134. (Original)The method of Claim 122, wherein said second agent reports on an address binding of a physical device identifier to a network address if the physical device identifier of a component was not previously known, or said network address in the address binding is a reassignment of said network address within a predetermined time period since said network address was last included in an address binding.

135. (Original)The method of Claim 122, wherein said second agent reports second data about a firewall, and said second data includes at least one of: a change to a saved firewall configuration corresponding to a predetermined threat level, a change to a current set of firewall configuration rules currently controlling operations between said industrial network and said other network.

136. (Original)The method of Claim 135, wherein log files associated with said firewall are stored remotely at a location on said second computer system with log files for said second computer system activity.

137. (Original)The method of Claim 122, wherein said second data includes at least one threat assessment from a source external to said industrial network.

138. (Original)The method of Claim 137, wherein said second data includes at least one of: a threat level indicator from a corporate network connected to said industrial network, a threat level indicator from a public network source, and a threat level indicator

that is manually input.

139. (Original) The method of Claim 121, further comprising:

receiving at least said first data by a receiver;

authenticating said first data as being sent by said first agent; and

processing, in response to said authenticating, said first data by said receiver.

140. (Original)The method of Claim 139, wherein said authenticating includes at least one of: verifying use of said first agent's encryption key, and checking validity of a message checksum, and using a timestamp or sequence number to detect invalid reports received by said receiver as being sent from said first agent.

141. (Original)The method of Claim 121, wherein said reporting is performed in accordance with a threshold size indicates an amount of data that said first agent is permitted to transmit in a fixed periodic reporting interval.

142. (Original)A computer program product for monitoring an industrial network comprising code that:

reports first data about a first computer system by a first agent executing on said first computer system in said industrial network, said first computer system performing at least one of: monitoring or controlling a physical process of said industrial network, said first data including information about software used in connection with said physical process.

143. (Original)The computer program product of Claim 142, further comprising code that:

reports second data about communications on a connection between said industrial network and another network by a second agent executing on a second computer system.

144. (Original)The computer program product of Claim 143, wherein said second data reported by said second agent is included in an appliance to which said first data is sent.

145. (Original)The computer program product of Claim 142, wherein said first agent reports on at least one of: critical file monitoring, log file for said first computer system, hardware and operating system of said first computer system, password and login, a specific application executing on said computer system wherein said application is in accordance with a particular industrial application of said industrial network.

146. (Original)The computer program product of Claim 145, wherein a plurality of agents execute on said first computer system monitoring said first computer system.

147. (Original)The computer program product of Claim 146, wherein said plurality of agents includes a master agent and other agents performing a predetermined set of monitoring tasks, said master agent controlling execution of said other agents.

148. (Original) The computer program product of Claim 147, wherein said plurality of agents report data at predetermined intervals to one of: an appliance and said second computer system.

149. (Original)The computer program product of Claim 148, further comprising code for performing, by at least one of said plurality of agents:

obtaining data from a data source;

parsing said data;

performing pattern matching on said parsed data to determine events of interest;

recording any events of interest;

reporting any events of interest in accordance with occurrences of selected events in a time interval;

creating a message including said summary at predetermined time intervals; and

encrypting at least one of: said message and a checksum of said message.

150. (Original) The computer program product of Claim 142, wherein said first data includes at least one of the following metrics: a number of open listen connections and a number of abnormal process terminations.

151. (Original)The computer program product of Claim 150, wherein, when a number of open listen connections falls below a first level, an event corresponding to a component failure is determined.

152. (Original)The computer program product of Claim 150, wherein, when a number of open listen connections is above a second level, an event corresponding to a new component or unauthorized component is determined.

153. (Original)The computer program product of Claim 143, wherein said second agent reports on network activity in accordance with a set of rules, said rules including at least one rule indicating that events in a business network are flagged as suspicious in said industrial network.

154. (Original)The computer program product of Claim 153, wherein said events include at least one of: an event associated with a web browser, and an event associated with e-mail.

155. (Original)The computer program product of Claim 143, wherein said second agent reports on an address binding of a physical device identifier to a network address if

the physical device identifier of a component was not previously known, or said network address in the address binding is a reassignment of said network address within a predetermined time period since said network address was last included in an address binding.

156. (Original) The computer program product of Claim 143, wherein said second agent reports second data about a firewall, and said second data includes at least one of: a change to a saved firewall configuration corresponding to a predetermined threat level, a change to a current set of firewall configuration rules currently controlling operations between said industrial network and said other network.

157. (Original) The computer program product of Claim 156, wherein log files associated with said firewall are stored remotely at a location on said second computer system with log files for said second computer system activity.

158. (Original)The computer program product of Claim 143, wherein said second data includes at least one threat assessment from a source external to said industrial network.

159. (Original)The computer program product of Claim 158, wherein said second data includes at least one of: a threat level indicator from a corporate network connected to said industrial network, a threat level indicator from a public network source, and a threat level indicator that is manually input.

160. (Original) The computer program product of Claim 142, further comprising code that:

receives at least said first data by a receiver;

authenticates said first data as being sent by said first agent; and

processes, in response to said code that authenticates, said first data by said receiver.

161. (Original)The computer program product of Claim 160, wherein said code that authenticates includes at least one of: code that verifies use of said first agent's encryption key and checks validity of a message checksum, and code that uses a timestamp or sequence number to detect invalid reports received by said receiver as being sent from said first agent.

162. (Original) The computer program product of Claim 142, wherein said code that reports uses a threshold size indicating an amount of data that said first agent is permitted to transmit in a fixed periodic reporting interval.

163. (Currently Amended)~~A method for detecting undesirable messages in a network comprising:~~

The method of Claim 121, wherein a second agent reports about communications within said industrial network, said second agent reporting on network activity in said industrial network in accordance with a set of rules, said rules including at least one rule defining an acceptable message, and the method further comprising:

receiving, by said second agent, a message ~~in said network~~;

determining if said message is undesirable in accordance with said at least one rule ~~defining an acceptable message in said network~~; and

reporting said message as undesirable if said message is not determined to be in accordance with said at least one rule.

164. (Original) The method of Claim 163, further comprising:

defining another rule for use in said determining if an additional message type is determined to be acceptable in said network.

165. (Currently Amended)~~A computer program product for detecting undesirable messages in a network comprising code that:~~

The computer program product of Claim 142, wherein a second agent reports about communications within said industrial network, said second agent reporting on network activity in said industrial network in accordance with a set of rules, said rules including at least one rule defining an acceptable message, and the computer program product further comprising code that:

receives, by said second agent, a message ~~in said network~~;

determines if said message is undesirable in accordance with said at least one rule defining an acceptable message ~~in said network~~; and

reports said message as undesirable if said message is not determined to be in accordance with said at least one rule.

166. (Original)The computer program product of Claim 165, further comprising code that:

defines another rule for use in said determining if an additional message type is determined to be acceptable in said network.

Claims 167. – 174. (Canceled)